UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/182,933	10/30/1998	GLENN ARTHUR REITMEIER	SAR13070	2555

28166 7590 05/03/2004

MOSER, PATTERSON & SHERIDAN, LLP
/SARNOFF CORPORATION
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER	
MEISLAHN, DOUGLAS J	

ART UNIT	PAPER NUMBER
2137	31

DATE MAILED: 05/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/182,933	Applicant(s) REITMEIER ET AL.	
	Examiner Douglas J. Meislahn	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18 and 22-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18 and 22-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 28 February 2004 that amended claims 1 and 24. The amendments have overcome the 112 rejection.

Response to Arguments

2. Applicant's arguments filed 28 February 2004 have been fully considered but they are not persuasive. After reprinting the first, fifteenth, twenty-third, and twenty-fourth claims, applicant generally describes the application's subject matter in the first paragraph of page 11. The examiner generally agrees with applicant's assessment of the instant invention. In the second paragraph of page 11, applicant describes the benefit of their invention, that being "multiple layers of protection" for an information stream. Adding layers of protection to sensitive information is always obvious because the addition better protects that sensitive information. As such the mere combination of protection layers cannot be the basis for the allowance of the instant claims.

3. In response to applicant's arguments against the references individually in the paragraph spanning pages 11 and 12 and the paragraph, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

4. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon

hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

5. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Kupnicki et al. and Inoue both teach methods of increasing the security of data, as mentioned in the rejection in the previous office action.

6. Applicant opines that the examiner fails to discuss the pending claims as a whole. Among others, item eight in the previous office action does, in fact, discuss the pending independent (and some dependent) claims in their entirety.

7. In response to applicant's argument that Kupnicki et al. and Inoue are nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443

(Fed. Cir. 1992). In this case, both are in the field of transmitted data protection. Kupnicki et al. and Inoue do not teach compression, as admitted by the examiner. However, nor do they teach against compression. As such, applicant's conclusion that they do so is in error.

8. Applicant's arguments for the patentability of dependent claims are based on their dependence from the independent claims. As shown above, the rejection of these claims is valid.

9. In the second full paragraph of page 16, applicant questions the applicability of Oshima et al. to the instant invention. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., sending, encrypting, and decrypting a key/index) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

10. Applicant notes that, in claim 23, the index is used after decryption, not for decryption. This is identical to the use of the key in the scrambling described by Oshima et al. in view of Inoue.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1, 2, 10-13, 15, and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. (5625416) in view of Kupnicki et al. (4742544) and Inoue (5195134).

In claim 1, Tseng et al. segment a video program, thereby meeting the limitations of the first clause of claim 1. As detailed in claim 4, the segments are compressed. According to claim 7, the compression is done to individual segments and thus after segmentation. MPEG, a prediction-based compression technique, is taught in lines 33-38 of column 1. As such, the limitations of the second clause of claim 1 are rendered obvious. Tseng et al. do not say that the segments are re-sequenced or encrypted. In their abstract, Kupnicki et al. teach randomly reordering segments of data in order to protect the data as a whole. Decryption data is used to reorder the re-sequenced data and thus corresponds to applicant's index. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to protect Tseng et al.'s segmented data by randomly re-sequencing it according to an index. Thus, the third clause of claim 1 is covered.

Encrypting data that has already been scrambled, although perhaps not a ubiquitous practice, is known in the art of data transmission, as evidenced by lines 18-22 of column 3 in Inoue; the encryption has the obvious advantage of providing increased security to the data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to increase security by encrypting Tseng et al.'s now-re-sequenced data as taught by Inoue.

An apparatus to produce this encrypted, scrambled, compressed data stream is inherent. A method to recover the data is anticipated as well.

With respect to claim 2, Inoue has taught encryption of the entire signal. Inoue also talks about subscribers in line 26 of column 3, thereby meeting the limitations of 2.

13. Claim 3, 6, 16, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claim 2 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. Control data for the mixing is also encrypted. They do not teach sending the control data to a receiver via a different medium. Official notice is taken that it is old and well known to send control data separately from the actual information. This is especially established in pay television systems; a card will be sent to a client, who puts the card in a machine on the client's television. The data on the card allows the descrambling of broadcast programming. This method provides a level of security by separating the scrambled data from the key to that data. All of the base references are concerned with data transmission, and therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to send control data by a different medium, such as a mailed card as is known in the art, the recipient in the combined system of Tseng et al. in view of Kupnicki et al. and Inoue. This would increase security.

14. Claims 4, 5, 17, 27, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claims 2, 3, 16, 25, and 26 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. They do not teach non-continuous temporal transmission. Official notice is taken that transmission of data, particularly encrypted data, in a non-continuous fashion is old and well known. By providing only part of a cryptogram, an attacker (probably) cannot decrypt any of the cryptogram. This is used in the interlock protocol, which, although concerned specifically with public keys, is applicable to symmetric cryptography. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to increase the security of Tseng et al. in view of Kupnicki et al. and Inoue by transmitting the data discontinuously. Also, if the data is transmitted as packets, it would inherently be transmitted discontinuously.

15. Claims 7, 8, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claims 1 and 28 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. There is no mention in either reference of the segments being a specific size or distributing the segments over many different distribution channels. Official notice is taken that digital broadcast over computer networks is old and well known as a method for data transmission. Data is generally

conveyed in packets that are generally the same size, meeting the limitations of claim 7. The networks use many different transmission paths to deliver data to a single source, meeting claim 29. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to apply the teachings of Tseng et al. in view of Kupnicki et al. and Inoue's joint transmission system to digital broadcast over networks.

16. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claim 1 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. They do not say that a non-predicted information segment is included in the segment. Official notice is taken that it is old and well known to include random information, such as an initialization vector, in data that is to be encoded. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include a non-predicted information frame within each segment of Tseng et al. in view of Kupnicki et al. and Inoue, thereby providing an initialization vector for the stream.

17. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claim 1 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. They do not say that the step of compressing produces control information indicative of a utilization level of a decoder buffer. This feature has been interpreted as being access rights for decompression. Official notice

is taken that access rights are an old and well-known type of control data that are used to indicate parties that are allowed to access a product. They are especially common in pay-television systems. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for commonly known access rights to be included in the control data of Tseng et al. in view of Kupnicki et al. and Inoue. The time of access rights generation is substantially inconsequential, but it would have been obvious to produce the rights at the same time as the operation that they control.

18. Claims 18 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tseng et al. in view of Kupnicki et al. and Inoue as applied to claim 15 above.

Tseng et al. in view of Kupnicki et al. and Inoue render obvious a system that compresses, mixes, and encrypts data. They do not specifically teach storing the unencrypted data in random access memory. Official notice is taken that it is old and well known that random access storage allows a processor to directly access data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use random access memory to store the data used in Tseng et al. in view of Kupnicki et al. and Inoue because the data is not accessed in the order in which it is meant to be viewed or heard.

19. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Oshima et al. (WO98/27553) (US 6266299 is an English-language equivalent) in view of the Microsoft Press *Computer Dictionary* and Inoue (5195134).

Figure 34 of Oshima et al. shows data being MPEG encoded (element 43) and scrambled by a scrambler (element 45) using a key (element 44). (For translation, see

English-language equivalent US 6266299 B1, figure 34 and the paragraph spanning columns 36 and 37). MPEG anticipates prediction-based compression, and the key corresponds to applicant's index. Oshima et al. do not say that the scrambling reorders data. The Microsoft Press Computer Dictionary (3rd ed.) defines a scrambler as a "device or program that reorders a signal sequence in order to render it indecipherable." As such, it would have been obvious to a person of ordinary skill in the art at the time the invention was made for Oshima et al.'s scrambler to reorder the MPEG-compressed data because, according to their definition, that is what scramblers do.

Oshima et al. do not encrypt the scrambled data. Encrypting data that has already been scrambled, although perhaps not a ubiquitous practice, is known in the art of data transmission, as evidenced by lines 18-22 of column 3 in Inoue; the encryption has the obvious advantage of providing increased security to the data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to encrypt the data on disks (element 240) pictured in figure 41 of Oshima et al. as taught by Inoue. This would increase security.

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Douglas J. Meislahn
Examiner
Art Unit 2137

DJM